REMARKS

Claims 1-31 are pending in the application. In this response, we have amended claims 15 and 16.

The examiner states that the effective filing date for the subject matter of the claims in the application is December 4, 2002. We note, however, that the application was actually filed on December 4, 2001, so the effective filing date is that earlier date.

The examiner rejected claim 14 under 35 U.S.C. §112, paragraph 1 as not complying with the enablement requirement. However, because claim 14 is an original claim, it is by definition part of the originally filed specification, and constitutes a clear disclosure of the claimed subject matter.

The examiner rejected claims 1-28 and 30-31 under 35 U.S.C. §103(a) as being unpatentable over Weiss (U.S. 4,885,778) in view of Kocher (U.S. 6,539,092). However, Weiss is missing several elements of the claims that Kocher does not supply. Further, the motivation the examiner provides for combining Weiss with Kocher would actually motivate one of skill in the art to use a different method than that recited in the claims.

The examiner admits that Weiss does not disclose first and second generation values, which are values indicative of a previous number of authentication code generations. The examiner argues that Kocher supplies these elements, in the form of transaction counter C. However, even if one assumes that transaction counter C is equivalent to first and second generation values, Weiss and Kocher do not teach or suggest using that value in the way required by claim 1. Specifically, Weiss and Kocher do not teach or suggest:

> ...generating an authentication code by combining the stored secret, the dynamic value, the first generation value, and the PIN...

The normal meaning of the word "combine" is to merge, or to bring into such close relationship as to obscure individual characters. The specification lists specific examples of combining that are consistent with this meaning:

> The combination of the secret (K) the dynamic value (T) and the generation value (N) may take place in any order and may use one or more various combination methods. For example, in one simplistic embodiment, the values (K, T, N) are EXCLUSIVE-ORed

> with each other to arrive at a resulting authentication code. In another embodiment, the values (K, T, N) are provided as input to a one-way function... ([0039]).

If one uses the word "combining" in the normal sense, one cannot reasonably consider that Weiss and Kocher teach or suggest generating an authentication code by combining a first generation value with a stored secret, dynamic value, or PIN, as required by claim 1.

Weiss discloses generating "non-predictable codes" by inputting a fixed code or seed, a pin, and a dynamic variable into a predetermined algorithm. Nowhere does Weiss teach or suggest combining any of these values with a first generation value.

Even if one assumes that transaction counter C is equivalent to a first generation value, Kocher does not teach or suggest generating an authentication code by combining that transaction counter C with any value. Instead, Kocher discloses updating a secret key K_C, by applying one of functions F_A, F_B, F_A^{-1}, or F_B^{-1} using a rule based on the value of C. To update K_C, Kocher first initializes a temporary counter variable V to the value of C, and then determines which function to apply to K_C using a rule based on the value of V.

> At step 230, the device tests whether the variable V is equal to the quantity 2^N-3. If equal, function F_A^{-1} should be applied, and processing proceeds to step 235 where the device increments C and updates K_C by computing $K_C \leftarrow F_A^{-1}(K_C)$. Otherwise, at step 240, the device tests whether the variable V is equal to the quantity $2(2^N-2)$. If equal, function F_B^{-1} should be applied... (col. 6, lines 8-14).

Kocher goes on to describe the rest of the rules, based on the value of V (i.e., C), for determining which one of the functions F_A, F_B, F_A^{-1}, or F_B^{-1} to apply to secret K_C (col. 6, lines 14-24). The examiner points to a specific application of one of the rules:

> [T]he secret value for transaction 117 is computed by applying the function K_B^{-1} to K_C.

Applying a selected function to K_C using a rule based on transaction counter C is not the same as generating an authentication code by combining a first generation value with a stored secret, dynamic value, and PIN, as recited in claim 1. Weiss and Kocher together do not teach or suggest combining a first generation value with any value.

Weiss is also missing other elements of claim 1, which Kocher does not supply. For example, Weiss does not teach or suggest:

generating a second generation value responsive to receipt of the PIN.

Weiss discloses two uses for a PIN. First, as described in the section cited by the examiner, Weiss uses a PIN to "guard against misappropriation of the fixed code/card seed" (col. 5, lines 20-22). To do this, Weiss compares the PIN "against a library of authentication card pins" to see if there is a match (col. 5, lines 34-36). Second, Weiss inputs the PIN to an algorithm for generating a non-predictable code:

> In order to generate a non-predictable code 40, FIGS. 1-3, which will ultimately give the user clearance or access, the fixed code or seed 10 and/or pin 45 must be input into a predetermined algorithm which manipulates the seed 10 and/or pin 45 as a static variable (col. 5, lines 44-49).

Comparing a PIN against a library of PINs, or using a PIN as a static variable in an algorithm, is not the same as generating a second generation value in response to receipt of a PIN, as recited in claim 1.

Kocher also does not teach or suggest this feature. Kocher discloses incrementing transaction counter C after a "transaction" (col. 5, lines 6-7), which the examiner appears to suggest involves "authentication associated with a PIN." However, Kocher does not teach or suggest a single transaction that uses a PIN. Instead, Kocher discloses transactions that use secret key K_C, not a PIN:

> computing or verifying a MAC (Message Authentication Code) on a message, encrypting or decrypting a message, producing a pseudo-random challenge value, deriving a key, etc" (col. 4, lines 42-46).

In other words, Kocher discloses incrementing transaction counter C after using secret key K_C. But this is not the same as generating a second generation value in response to receipt of a PIN, as required by claim 1.

Additionally, the examiner provides a motivation for combining Weiss and Kocher that would actually motivate one to produce a different invention than that which is claimed. The examiner argues that it would be obvious to combine the systems of Weiss and Kocher because:

> Kocher teaches providing a fast and efficient method for obtaining leak-resistance and leak-proof security mechanism during the authentication of the new session communications.

But Kocher discloses achieving this by repeatedly updating secret K_C with function F_A, F_B, F_A^{-1}, or F_B^{-1}, at a client computer. This allows the secret to be reused only a limited number of times, while improving the performance of a corresponding server computer.

> The present invention can include a sequence of client-side updating processes that allow for significant improvements in the performance of the corresponding server operations, while maintaining leak-resistant and/or leak-proof security characteristics in the client device (col. 2, lines 54-58).
>
> [S]uch update functions are applied by the client in a sequence that assures that any single secret value is never used or derived more than a fixed number of times (for example, three) (col. 2, lines 62-65).

So, based on Kocher, one would be motivated to update a secret by applying a function or sequence of functions to the secret, at a client computer. But combining these features with Weiss does not reproduce the invention of claim 1.

For at least the reasons given above, we submit that claim 1, and the claims dependent thereon, is not obvious over Weiss in view of Kocher.

For similar reasons, claim 17 is not obvious over Weiss in view of Kocher. For example, Weiss and Kocher do not teach or suggest "calculating a second generation value responsive to receipt of the PIN by the PIN subsystem," as recited in claim 17. Weiss discloses comparing a PIN to a PIN library, and using a PIN as a static variable in an algorithm, which is not the same as calculating a second generation value in response to receipt of a PIN. Kocher discloses incrementing transaction counter C after transactions that use secret key K_C, but these transactions do not involve receiving a PIN. There is no suggestion in the combined references to calculate a second generation value in response to receipt of a PIN, as recited in claim 17.

Additionally, regarding claim 17, Weiss and Kocher do not teach or suggest:

> a combination subsystem generating an authentication code by retrieving the secret from the memory element and combining the secret and the dynamic value from the dynamic value subsystem, the PIN received by the PIN subsystem, and the generation value from the generation value subsystem.

As discussed above, there is no teaching or suggestion in Weiss to combine a generation value with any other value. Therefore, Weiss also does not teach or suggest a subsystem for performing this function. Also, as discussed above, Kocher does not teach or suggest <u>combining</u>

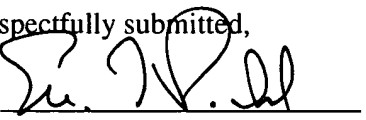
a generation value with any other value. Thus, Kocher does not teach or suggest a combination subsystem that performs this function.

Therefore, we submit that claim 17, and the claims dependent thereon, is not obvious over Weiss in view of Kocher.

For at least these reasons, applicants believe the pending application is in condition for allowance. A petition for a one-month extension of time accompanies this response, and the Commissioner is hereby authorized to charge the required fee of $60 for filing the petition to Deposit Account No. 08-0219. No other fees are believed to be due at this time. However, please charge any fees, or credit any overpayments, to Deposit Account No. 08-0219.

Dated: March 14, 2006

Respectfully submitted,

By 

Eric L. Prahl
Registration No.: 32,590
WILMER CUTLER PICKERING HALE AND DORR LLP
60 State Street
Boston, Massachusetts 02109
(617) 526-6000
Attorney for Applicant